UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,005	01/07/2002	David E. Halasz	72255/08267	4708

23380 7590 03/19/2007

TUCKER, ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/041,005	HALASZ ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *71-100* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *71-100* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 71-100 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 71-100 are rejected under 35 U.S.C. 102(e) as being anticipated by Juitt et al. U.S. Pat. No. 7042988 (hereinafter Juitt).

4. As per claim 71, Juitt discloses a system, comprising: an authentication server disposed on a network (Juitt: figure 1A: authentication server 125); a switch coupled to the network and communicatively coupled to the authentication server via the network (Juitt: figure 1A: gateway server 120); and an access point communicatively coupled to the switch (Juitt: figure 1A: access points 102a-c); wherein the access point is configured to authenticate with the authentication server and establish a secure communication session with the switch (Juitt: column 8 lines 39-42: authentication between gateway server and access points; column 14 lines 4-11: gateway server can detect rogue access points by utilizing MAC of access points); wherein the access point is configured to send a message to the switch comprising data representative of an authenticated wireless client responsive to the authenticated wireless client successfully authenticating with the authentication server (Juitt: column 9 lines 27-52: forwarding request to the gateway server...request can include identifier); and wherein the access point is configured

to forward all communications received from the authenticated wireless client to the switch responsive to the authenticated wireless client successfully authenticating with the authentication server (Juitt: figure 1A: all requests have to go through access points to gateway server; figure 2: provide access upon authentication).

5. As per claim 72, Juitt discloses the system according to claim 71. Juitt further discloses the switch comprises a table of authorized users, wherein the switch updates the table of authorized users with the medium access control address of the authenticated wireless client (Juitt: column 11 lines 19-43: internal authentication database; column 13 lines 6-13: MAC).

6. As per claim 73, Juitt discloses the system according to claim 71. Juitt further discloses the switch comprises a table of authorized users, wherein the switch updates the table of authorized users with the medium access control list, the quality of service parameters and the access control list of the authenticated wireless client (Juitt: column 11 lines 19-43: maintains a internal database for authentication of authenticated users).

7. As per claim 74, Juitt discloses the system according to claim 71. Juitt further discloses wherein a session key is generated for subsequent communications between the authenticated wireless client and the access point responsive to the authenticated wireless client successfully authenticating with the authentication server (Juitt: column 7 lines 39-41: WEP data encryption).

8. As per claim 75, Juitt discloses the system according to claim 71. Juitt further discloses the system comprising the authentication server is responsive to establish a message authentication check key for the secure communication session between the switch and the access point (Juitt: column 6 lines 38-

41: 802.11 protocol supports message authentication code for communications; column 7 lines 36-42: gateway server and access points can communicate using any well known communication protocols used between access points and wireless clients such as the 802.11).

9. As per claim 76, Juitt discloses the system according to claim 75. Juitt further discloses wherein the message authentication check key uniquely identifies the access point to the switch (Juitt: column 7 lines 39-41).

10. As per claim 77, Juitt discloses the system according to claim 75. Juitt further discloses the system comprising:

the access point is configured to send the data representative of the authenticated wireless client signed with the message authentication check key (Juitt: column 7 lines 36-41; column 8 lines 39-44: communication between access point and gateway server is protected); and

the switch is responsive to receiving the data representative of the authenticated wireless client to verify the message authentication check key (Juitt: column 8 lines 39-44: authenticate packets from access points).

11. As per claim 78, Juitt discloses the system according to claim 77. Juitt further discloses the system comprising:

the switch is configured to maintain a database containing authorized media access control addresses (Juitt: column 11 lines 19-44: internal database; column 13 lines 10-12: authentication information includes MAC); and

the switch is configured to verify the message with the data representative of the authenticated wireless client was sent by the access point by verifying the media access control

address of the access point (Juitt: column 14 lines 1-11: detect rogue access points by looking for MAC).

12. As per claim 79, Juitt discloses the system according to claim 78. Juitt further discloses the system comprising:

the data representative of the authenticated wireless client comprises a media access control address for the authenticated wireless client (Juitt: column 9 lines 25-42: access point forward requests to gateway server... request include identifier and authentication information; column 13 lines 10-12: authentication information includes MAC address);

the switch is responsive to receiving the data representative of the authenticated wireless client to store the media access control address for the authenticated wireless client in the database (Juitt: column 11 lines 25-44: internal authentication database maintains authentication information of authenticated users); and

the switch is responsive to receiving packets from the authenticated wireless client forwarded by the access point to verify the media access control address of the packets from the authenticated wireless client with the database (Juitt: column 13 lines 6-12).

13. As per claim 80, Juitt discloses the system according to claim 71. Juitt further discloses wherein the secure communication session is established between the switch and the access point prior to authenticating the authenticated wireless client (Juitt: column 14 lines 1-11).

14. As per claim 81, Juitt discloses the system according to claim 71. Juitt further discloses the system comprising: the switch maintains a database of authenticated supplicants (Juitt: column 11 lines 30-44); and the switch stores the media access control of the access point in the database responsive to the access point successfully authenticating with the authentication server (Juitt: column 13 lines 10-12).

15. As per claim 82, Juitt discloses a system, comprising: an authentication server disposed on a network (Juitt: figure 1A: authentication 125); a first authenticator communicatively coupled to the authentication server via the network (Juitt: figure 1A: gateway server 120); and a first supplicant communicatively coupled to the first authenticator (Juitt: figure 1A: access points 102a-c); wherein the first supplicant is configured to authenticate with the authentication server and establish a secure communication session with the first authenticator (Juitt: column 14 lines 1-11); wherein the first supplicant is configured to function as an authenticator for a second supplicant communicatively coupled to the first supplicant (Juitt: figure 1A: access points 102 and mobile device 100); wherein the first supplicant is configured to send a message with data representative of the second supplicant to the first authenticator responsive to the second supplicant successfully authenticating with the authentication server (Juitt: column 9 lines 27-52: forwarding request to the gateway server...request can include identifier); and wherein the first supplicant is configured to forward all communications received from the second supplicant to the first authenticator responsive to the second supplicant successfully authenticating with the authentication server (Juitt: figure 1A: all requests have to go through access points to gateway server; figure 2: provide access upon authentication).

16. As per claim 83-100, claims 83-100 disclose the same limitations as claims 71-82. Therefore, claims 83-100 are rejected based on the same reasons set forth above in rejecting claims 71-82.

Response to Arguments

17. Applicant's arguments with respect to claims 71-100 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100